

REMARKS

The comments of the applicant below are each preceded by related comments of the examiner (in small, bold type).

Claim 40 rejected under 35 U.S.C. 102(e) as being anticipated by Lyle, U.S. Patent No. 6,886,102.

**...
Claims 1-2, 6-8, 9-10, 14-22, 28-34 and 41, 45, 46, 48 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack), U.S. Patent No. 6,298,445 in view of Lyle, U.S. Patent No. 6,886,102 and further in view of Shipley, U.S. Patent No. 6,119,236.**

Shostack and Lyle do not disclose and would not have suggested determining in real time an existence of an anomaly based on the indications of the possible security problems from at least two remote clients, in which the anomaly is not apparent from analyzing the possible security problem or problems at only one of the remote clients, as recited in amended claim 40.

Shostack does not disclose analyzing the possible security problems at two or more client locations. Although Lyle discloses sniffers that provide information concerning suspicious data (col. 7, lines 15-17) and processing the suspicious data, Lyle does not disclose determining "in real time" an existence of an anomaly based on the indications of the possible security problems from at least two remote clients, in which "the anomaly is not apparent from analyzing the possible se

Claims 1, 9, 17, 28, 30, 41 are patentable for at least similar reasons as those applied to claim 40.

Claims 42 and 52 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) and further in view of Moran, U.S. Patent No. 6,826,697.

As per claim 42: Shostack discloses a method comprising: detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem); transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server); transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly). Shostack fails to teach determining at the home location an anomaly by at least comparing the possible security problem with information previously logged at the home location, including searching for an unexpected login. However, Lyle discloses a method

wherein the event, which consists of an attack, is compared to other events that have occurred (7:50-8:11).

Shostack and Lyle fail to teach a method in which determining the anomaly comprises searching for an unexpected login. However, Moran discloses a method wherein failed login attempts are logged (19:41-20:18). A failed login attempt is an unexpected login since it is not a correct login. The login is not expecting for the login information to be wrong, therefore a failed login qualifies as an unexpected login by an unexpected user. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with Moran because in order to make a system less vulnerable to attack as stated in Shostack (2:18- 28), the ability to detect further types of attacks such as forward and backward time steps in a log file or an overflow buffer attack as stated in Moran (4:1-37) would increase the security against attacks as a whole.

Moran does not disclose and would not have suggested searching for a "successful but unexpected login," as recited in claim 42. What Moran discloses is logging failed login attempts. A "failed" login attempt is an attempt to login that failed. A "failed" login attempt is not a "successful" but unexpected login, as recited in claim 42.

All of the dependent claims are patentable for at least similar reasons as those for the claims on which they depend are patentable.

Any circumstance in which the applicant has addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner. Any circumstance in which the applicant has made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims. Any circumstance in which the applicant has amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Applicant : David W. Auesmith et al.
Serial No. : 10/010,743
Filed : December 6, 2001
Page : 12 of 12

Attorney's Docket No.: 10559-463001 / P10875

Please apply \$50 to excess claims fee and any other charges or credits to deposit
account 06-1050, reference 10559-463001.

Respectfully submitted,

Date: January 18, 2007

/Rex I. Huang/

Rex I. Huang
Reg. No. 57,661

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21501425.doc